PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344368
(43)Date of publication of application : 14.12.2001

(51)Int.CI. G06F 17/60
G09C 1/00

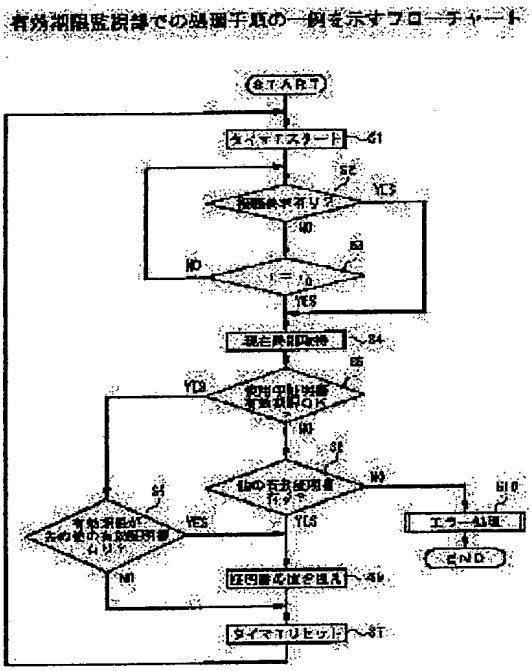
(21)Application number : 2001-093813
(22)Date of filing : 28.03.2001

(71)Applicant : FUJITSU LTD
(72)Inventor : OKAZAKI KOTARO

(30)Priority
Priority number : 2000099378 Priority date : 31.03.2000 Priority country : JP

(54) MANAGEMENT METHOD, DEVICE, PROGRAM AND STORAGE MEDIUM FOR ELECTRONIC CERTIFICATE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a management method and a device for electronic certificate which can alter the electronic certificate while keeping operation of a service-providing server.
SOLUTION: This above task is accomplished by the management method and the device for electronic certificate such that a service-providing server manages electronic certificate to be used for authentication, also manages an electronic certificate to be reserved without being used, at a prescribed timing, alters the management of an electronic certificate that is reserved, without being used for authentication into the management as the electronic certificate to be used for authentication, and also alters the management of electronic certificate to be used for the authentication into the management of electronic certificate that is reserved, without its being used for the authentication.



LEGAL STATUS

[Date of request for examination] 19.12.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－344368
（P2001－344368A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	１４０	Ｇ０６Ｆ　17/60	１４０	
	ＺＥＣ		ＺＥＣ	
	５１２		５１２	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	

審査請求　未請求　請求項の数11　ＯＬ　（全 13 頁）

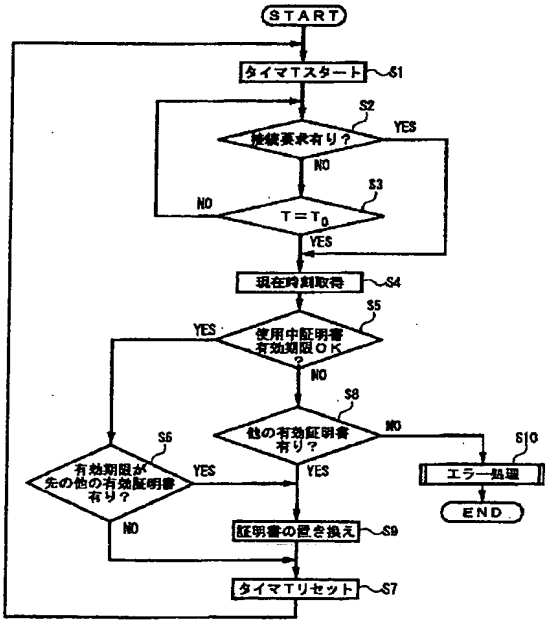
(21)出願番号　特願2001－93813(P2001－93813)
(22)出願日　平成13年３月28日(2001.3.28)
(31)優先権主張番号　特願2000－99378(P2000－99378)
(32)優先日　平成12年３月31日(2000.3.31)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岡崎　耕太郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100070150
弁理士　伊東　忠彦

(54)【発明の名称】　電子証明書の管理方法、装置、プログラム及び記憶媒体

(57)【要約】
【課題】サービス提供サーバの運用を継続した状態で電子証明書の変更を行うことのできる電子証明書の管理方法及び装置を提供することである。
【解決手段】上記課題は、サービス提供サーバは、認証に使用されるべき電子証明書を管理すると共に、認証に使用されることなく保存される電子証明書を管理し、所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するようにした電子証明書の管理方法及び装置にて達成される。

有効期限監視部での処理手順の一例を示すフローチャート



1

【特許請求の範囲】

【請求項1】接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理方法において、

サービス提供サーバは、

認証に使用されるべき電子証明書を管理すると共に、

認証に使用されることなく保存される電子証明書を管理し、

所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するようにした電子証明書の管理方法。

【請求項2】接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理装置において、

認証に使用されるべき電子証明書を管理すると共に、認証に使用されることなく保存される電子証明書を管理する証明書管理手段と、

所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するように上記証明書管理手段における電子証明書の管理の変更制御を行う管理変更制御手段とを有する電子証明書の管理装置。

【請求項3】請求項2記載の電子証明書の管理装置において、

上記証明書管理手段は、有効期間内でその期限に達する前の電子証明書を認証に使用されるべき電子証明書として管理すると共に、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の開始時より遅い開始時となる有効期間の電子証明書を認証に使用されることなく保存された電子証明書として管理するようにし、

上記管理変更制御手段は、認証に使用されるべき電子証明書として管理される電子証明書の有効期限が切れたか否かを判定する有効期限判定手段を有し、

認証に使用されるべき電子証明書として管理される電子証明書の有効期限が切れたと上記有効期限監視手段が判定したときに、上記電子証明書の管理の変更を行うようにした電子証明書の管理装置。

【請求項4】請求項3記載の電子証明書の管理装置において、

上記有効期限判定手段は、所定周期にて当該電子証明書の有効期限が切れているか否かを判定するようにした電子証明書の管理装置。

2

【請求項5】請求項3または4記載の電子証明書の管理装置において、

上記有効期限判定手段は、クライアント端末から上記サービス提供サーバに対して接続要求が成される毎に当該電子証明書の有効期限がきれているか否かを判定するようにした電子証明書の管理装置。

【請求項6】請求項2記載の電子証明書の管理装置において、

上記証明書管理手段は、有効期間内でその期限に達する前の電子証明書を認証に使用されるべき電子証明書として管理すると共に、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の開始時より遅い開始時となる有効期間の電子証明書を認証に使用されることなく保存された電子証明書として管理するようにし、

上記管理変更制御手段は、有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されているか否かを判定する判定手段を有し、

上記有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されていると上記判定手段が判定したときに、上記電子証明書の管理の変更を行うようにした電子証明書の管理装置。

【請求項7】請求項6記載の電子証明書の管理装置において、

上記判定手段は、所定周期にて有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されているか否かを判定するようにした電子証明書の管理装置。

【請求項8】請求項6または7記載の電子証明書の管理装置において、

上記判定手段は、クライアント端末から上記サービス提供サーバに対して接続要求が成される毎に有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されているか否かを判定するようにした電子証明書の管理装置。

【請求項9】請求項2乃至8いずれか記載の電子証明書の管理装置において、

上記証明書管理手段にて認証に使用されることなく保存される電子証明書として管理されるべき電子証明書を追加する証明書追加手段を有する電子証明書の管理装置。

【請求項10】接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理方法に従った処理をコンピュータに行わせるためのプログラムにおいて、

認証に使用されるべき電子証明書が管理されると共に、認証に使用されることなく保存される電子証明書が管理される状況で、

所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するように上記電子証明書の管理の変更制御を行う 管理変更制御手順を有するプログラム。

【請求項11】請求項10記載のプログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子証明書の管理方法及び装置係り、詳しくは、接続要求のあったクライアント端末にて対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理方法及び装置に関する。

【0002】上記電子証明書の管理方法に従った処理をコンピュータに行わせるためのプログラム及びそれを記憶した記憶媒体に関する。

【0003】

【従来の技術】近年、インターネットを利用した電子商取引が広く行われるようになり、世界中のどこからでも、また、いつでも商取引を行うことができるようなシステムが提案されている。このようなインターネットを利用した電子商取引に際してなされる情報通信を保護するためのプロトコルとして、Netscape社が提唱したＳＳＬ（Secure Sockets Layer）プロトコルがある。

【0004】このＳＳＬプロトコルを用いた情報通信を行うには所定の認証局が発行した電子証明書（以下、単に証明書ともいう）が必要となる。従って、ＳＳＬプロトコルを用いてクライアント端末と情報通信を行ってユーザに対してサービス（商取引など）を提供するサービス提供サーバ（以下、ＳＳＬサーバともいう）は、認証局が発行した当該ＳＬＬサーバを保証する証明書を保有することになる。この証明書には、発行者（認証局）名、サーバ（ＳＳＬサーバ）名、公開鍵、署名などの情報が記述されると共にその有効期限が設定されている。

【0005】ユーザは、クライアント端末を上記のようなＳＳＬサーバに接続して、当該ＳＬＬサーバからインターネットを介してサービスの提供を受ける。その際、クライアント端末（実際にはクライアント端末のブラウザ）とＳＳＬサーバとの間で情報通信を行い、クライアント端末にて上記証明書に基づいてサービスの提供元であるサーバが正規のＳＳＬサーバであることの確認、即ち、認証確認を行う。このような認証確認により、サーバの成りすましによる不正商取引や盗聴、情報改ざんなどを防止することができ、安全な情報通信（電子商取引など）が保証される。

【0006】ところで、上記証明書の有効期限が切れた場合、ＳＳＬサーバの認証確認をすることができず、ＳＳＬプロトコルを用いた情報通信ができなくなる。このため、ＳＳＬサーバの管理者は、証明書の有効期限が近づくと、認証局から新たな有効期限の証明書を発行してもらう。そして、使用していた証明書の有効期限になると、ＳＳＬサーバを一端停止させ、当該サーバ内の証明書を新たに発行された証明書に置き換えた後に、当該ＳＳＬサーバの運用を再開するようにしている。

【0007】

【発明が解決しようとする課題】上記のように、証明書の有効期限になった場合に、サービス提供サーバを一端停止させて、新たな証明書に置き換えるようにする従来の電子証明書の管理方法では、サービス提供の中断状態が生じ、あらゆる時刻になされる要求に対して常にサービスを提供することができない。

【0008】そこで、本発明の第一の課題は、サービス提供サーバの運用を継続した状態で電子証明書の変更を行うことのできる電子証明書の管理方法及び装置を提供することである。

【0009】また、本発明の第二の課題は、そのような電子証明書の管理方法に従った処理をコンピュータに行わせるためのプログラム及びそれを格納した記憶媒体を提供することである。

【0010】

【課題を解決するための手段】上記第一の課題を解決するため、本発明は、請求項1に記載されるように、接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理方法において、サービス提供サーバは、認証に使用されるべき電子証明書を管理すると共に、認証に使用されることなく保存される電子証明書を管理し、所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するように構成される。

【0011】このような電子証明書の管理方法では、サービス提供サーバは、認証に使用されるべき電子証明書を管理すると共に認証に使用されることなく保存される電子証明書を管理する。この状態で、認証に使用されるべき電子証明書として管理される電子証明書を用いてサービス提供サーバの上記運用が開始された後の所定タイミングで、その運用が継続された状態で、上記認証に使用されることなく保存される電子証明書の管理が上記認証に使用されるべき電子証明書としての管理に変更され

5

る。すると、以後、クライアント端末からの接続要求があったときには、上記のように認証に使用されるべき電子証明書として管理に変更された電子証明書を用いてサービス提供サーバの運用が行われる。

【００１２】上記所定のタイミングは、認証に使用されるべき電子証明書と、認証に使用されることなく保存される電子証明書との有効性の継続性が保たれる状態では、少なくとも認証に使用されることなく保存された電子証明書が有効となる任意のタイミングに定めることができる。

【００１３】各電子証明書の有効期間に基づいた管理を実現するという観点から、本発明は、上記電子証明書の管理方法において、有効期間内でその期限に達する前の電子証明書を認証に使用されるべき電子証明書として管理すると共に、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の開始時より遅い開始時となる有効期間の電子証明書を認証に使用されることなく保存された電子証明書として管理し、上記使用されることなく保存される電子証明書として管理される電子証明書の有効期間の開始タイミングで、上記電子証明書の管理の変更を行うように構成することができる。

【００１４】上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の期限と、上記認証に使用されることなく保存される電子証明書として管理される電子証明書の有効期間の開始タイミングが時間的に連続している場合、認証に使用されるべき電子証明書として管理される電子証明書の有効期限が切れた直後に、認証に使用されることなく保存される電子証明書として管理されていた電子証明書が認証に使用されるべき電子証明書として管理されるようになる。また、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間と、上記認証に使用されることなく保存される電子証明書として管理される電子証明書の有効期間がオーバーラップする場合、上記認証に使用されるべき電子証明書として管理されていた電子証明書の有効期限が切れる前に、上記認証に使用されることなく保存される電子証明書として管理されていた電子証明書の有効期限の開始タイミングにて当該電子証明書の管理の変更がなされる。

【００１５】また、上記第一の課題を解決するため、本発明は、請求項2に記載されるように、接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理装置において、認証に使用されるべき電子証明書を管理すると共に、認証に使用されることなく保存される電子証明書を管理する証明書管理手段と、所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書

6

の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するように上記証明書管理手段における電子証明書の管理の変更制御を行う管理変更制御手段とを有するように構成される。

【００１６】電子証明書の有効期間に基づいた管理を行う際に、認証に使用されるべき電子証明書として管理されていた電子証明書の有効期限が切れたときに即座に認証に使用されるべき電子証明書を用意できるという観点から、本発明は、請求項3に記載されるように、上記電子証明書の管理装置において、上記証明書管理手段は、有効期間内でその期限に達する前の電子証明書を認証に使用されるべき電子証明書として管理すると共に、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の開始時より遅い開始時となる有効期間の電子証明書を認証に使用されることなく保存された電子証明書として管理するようにし、上記管理変更制御手段は、認証に使用されるべき電子証明書として管理される電子証明書の有効期限が切れたか否かを判定する有効期限判定手段を有し、認証に使用されるべき電子証明書として管理される電子証明書の有効期限が切れたと上記有効期限監視手段が判定したときに、上記電子証明書の管理の変更を行うように構成することができる。

【００１７】上記有効期限判定手段は、請求項4に記載されるように、所定周期にて当該電子証明書の有効期限が切れているか否かを判定するように構成することができる。

【００１８】上記所定周期は、予想されるクライアント端末からの接続要求の頻度等に基づいて適当な値に定められる。

【００１９】また、クライアント端末からの接続要求に対して、サービス提供サーバの認証に使用される電子証明書を確実に用意できるという観点から、上記有効期限判定手段は、請求項5に記載されるように、クライアント端末から上記サービス提供サーバに対して接続要求が成される毎に当該電子証明書の有効期限がきれているか否かを判定するように構成することができる。

【００２０】また、電子証明書の有効期間に基づいた管理を行う際に、認証に使用されることなく保存される電子証明書として管理されていた電子証明書の有効期間の開始タイミングにて即座に認証に使用されるべき電子証明書を用意できるという観点から、本発明は、請求項6に記載されるように、上記電子証明書の管理装置において、上記証明書管理手段は、有効期間内でその期限に達する前の電子証明書を認証に使用されるべき電子証明書として管理すると共に、上記認証に使用されるべき電子証明書として管理される電子証明書の有効期間の開始時より遅い開始時となる有効期間の電子証明書を認証に使用されることなく保存された電子証明書として管理するようにし、上記管理変更制御手段は、有効期間の開始タイミングとなった電子証明書が上記証明書管理手段によ

り認証に使用されることなく保存される電子証明書として管理されているか否かを判定する判定手段を有し、上記有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されていると上記判定手段が判定したときに、上記電子証明書の管理の変更を行うように構成することができる。

【００２１】上記判定手段は、請求項7に記載されるように、所定周期にて有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されているか否かを判定するようにすることも、また、請求項8に記載されるように、クライアント端末から上記サービス提供サーバに対して接続要求が成される毎に有効期間の開始タイミングとなった電子証明書が上記証明書管理手段により認証に使用されることなく保存される電子証明書として管理されているか否かを判定するようにすることもできる。

【００２２】本発明は、更に、請求項9に記載されるように、上記各電子証明書の管理装置において、証明書管理手段にて認証に使用されることなく保存される電子証明書として管理されるべき電子証明書を追加する証明書追加手段を有するように構成することができる。

【００２３】また、本発明は、上記各電子証明書の管理装置において、上記管理変更制御手段により上記認証に使用されるべき電子証明書としての管理から上記認証に使用されることなく保存される電子証明書としての管理に変更された電子証明書を上記証明書管理手段での管理の対象から削除する証明書削除手段を有するように構成することができる。

【００２４】上記第二の課題を解決するため、本発明は、請求項１０及び請求項１１に記載されるように、接続要求のあったクライアント端末に対して所定のネットワークを介してサービスの提供を行うように運用されるサービス提供サーバの認証に用いられる電子証明書の管理方法に従って処理をコンピュータに行わせるためのプログラムにおいて、認証に使用されるべき電子証明書が管理されると共に、認証に使用されることなく保存される電子証明書が管理される状況で、所定のタイミングで、上記認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するように上記電子証明書の管理の変更制御を行う管理変更制御手順を含むプログラム、及びそれを格納した記憶媒体のように構成される。

【００２５】上記記憶媒体は、コンピュータが読取可能な媒体であれば特に限定されず、例えば、ＣＤ－ＲＯＭ、磁気ディスク、光磁気ディスク（ＭＯ）、フロッピー（登録商標）ディスク、磁気テープ、半導体メモリなどの記憶媒体を用いることができる。

【００２６】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

【００２７】本発明の実施の一形態に係る電子証明書の管理方法が適用されるシステムの基本的な構成は、例えば、図1に示すようになっている。

【００２８】図1において、所定のネットワーク５０（インターネットなど）を介して各クライアント端末２０（１）、２０（２）、…、２０（ｎ）は、ＳＳＬサーバ（サービス提供サーバ）１０からサービスの提供（電子商取引など）を受けることができる。そのサービスの提供に際して、ＳＳＬサーバ１０とクライアント端末２０（ｉ）との間では、ＳＳＬプロトコルに従った認証処理が行われる。ＣＡ局３０（認証局）は、この認証処理に用いられるＳＳＬサーバ１０を保証するための証明書を当該ＳＳＬサーバ１０に対して発行する。この証明書は、ＣＡ局３０からネットワーク５０を介して電子メールの形式でＳＳＬサーバ１０に提供することも、また、証明書を記憶した媒体を郵送などによってＳＳＬサーバ１０に提供することもできる。

【００２９】上記ＳＳＬサーバ１０の基本的なハードウエア構成は、例えば、図2に示すようになっている。

【００３０】図2において、このＳＳＬサーバ１０は、それぞれバスに接続されたＣＰＵ（中央演算処理ユニット）１１０、メモリユニット１２０、表示ユニット１３０、入力ユニット１４０、通信ユニット１５０、補助記憶ユニット１６０及びＣＤ－ＲＯＭドライバユニット１７を有している。

【００３１】ＣＰＵ１１０は、メモリユニット１２０に格納されたプログラムに従ってサービス提供に係る処理、証明書の管理処理等の各種処理を行うと共に当該サーバ内の各ユニットの制御を行う。メモリユニット１２０は、ＲＡＭ、ＲＯＭを有し、ＣＰＵ１０にて実行されるプログラムやデータ等を記憶する。表示ユニット１３０は、ＣＰＵ１０の制御に基づいて、各種の情報を表示する。入力ユニット１４０は、ユーザ（管理者）によって操作され、各種のコマンドを入力するために使用される。通信ユニット１５０は、ネットワーク１５０を介して他の通信装置（各クライアント２０（１）、２０（２）、…、２０（ｎ）やＣＡ局３０など）とデータ通信を行う。補助記憶ユニット１６０は、例えば、ディスク装置で構成され、プログラム、管理テーブル、ファイル、更にＣＡ局３０から発行された証明書などを格納する。

【００３２】証明書の管理処理に係るプログラム等の各種プログラムは、ＣＤ－ＲＯＭ１８０にて当該ＳＳＬサーバ１０に提供される。各種プログラムを格納したＣＤ－ＲＯＭ１８０がＣＤ－ＲＯＭドライバユニット１７０

9

にセットされると、ＣＤ－ＲＯＭドライバユニット１７０がＣＤ－ＲＯＭ１８０から各種プログラムを読み出し、その読み出されたプログラムが補助記憶ユニット１６０にインストールされる。そして、実行すべきプログラムは、補助記憶ユニット１６０から読み出されてメモリユニット１２０に格納される。

【００３３】ＣＡ局３０は、例えば、図3に示すように階層的に位置付けのなされた各種証明書を発行する。最上位の層に位置する証明書は、ＣＡ局３０自身を保証するためのＣＡ局証明書Ｒであり、その下層に位置する証明書は、ＳＳＬサーバ１０を保証するためのサーバ証明書Ｓ、各クライアント端末２０（１）、２０（２）、…、２０（ｎ）を保証するためのクライアント証明書Ａ、Ｂ、…となる。このように階層的に位置付けのなされた各種証明書は、最上位の証明書であるＣＡ証明書Ｒの情報を用いて下位層のサーバ証明書Ｓ及び各クライアント証明書Ａ、Ｂ、…の検証を行うことができるようになっている。

【００３４】ＣＡ局３０から発行されたサーバ証明書Ｓは、ＣＡ証明書Ｒと共にＳＳＬサーバ１０（補助記憶ユニット１６０）に保存される。また、例えば、各クライアント端末２０（１）、２０（２）、…、２０（ｎ）のブラウザには、そのブラウザの供給元とＣＡ局３０の運営会社との契約に基づいて、ＣＡ局証明書Ｒが予め埋め込まれている。そして、ＣＡ局３０から発行される各クライアント証明書Ａ、Ｂ、…が対応するクライアント端末２０（１）、２０（２）、…、２０（ｎ）に保存される。このように、ＳＳＬサーバ１０と各クライアント端末２０（１）、２０（２）、…、２０（ｎ）にＣＡ証明書Ｒが保存されることにより、ＳＳＬサーバ１０及び各クライアント端末２０（１）、２０（２）、…、２０（ｎ）では、そのＣＡ証明書Ｒを用いて相互に通信相手の証明書の検証を行うことができる（相互認証）。

【００３５】ＣＡ局３０では、次のようにして各証明書が作成される。

【００３６】図4に示すように、ＣＡ証明書Ｒは、主体者Ｒ名、公開鍵R_{kp}、発行者Ｒ名（例えば、ＣＡ局３０の運営会社名）、住所、電話番号などの被証明者Ｒ（主体者Ｒ）に関する情報が記述された証明書本体と電子署名にて構成される。この電子署名は、証明書本体の情報を所定のアルゴリズムに従ってハッシュ処理してダイジェストを生成し、そのダイジェストを当該ＣＡ局３０の秘密鍵R_{ks}にて暗号化することにより作成される。

【００３７】また、サーバ証明書Ｓも、ＣＡ証明書Ｒと同様に、主体者Ｓ名（サーバ名）、公開鍵S_{kp}、発行者Ｒ名（例えば、ＣＡ局の運営会社名）、住所、電話番号等の被証明者Ｓ（主体者Ｓ）に関する情報が記述された証明書本体と電子署名にて構成される。この電子署名も、上記ＣＡ証明書Ｒの場合と同様に、証明書本体の情報を所定のアルゴリズムに従ってハッシュ処理してダイジェストを生成し、そのダイジェストをＣＡ局の秘密鍵R_{ks}にて暗号化することにより作成される。

10

【００３８】また、ＣＡ局３０から発行される各証明書には、その有効期間が設定されている。

【００３９】クライアント端末２０（ｉ）は、ＳＳＬサーバ１０からサービスの提供を受ける場合、ネットワーク５０を介して当該ＳＳＬサーバ１０に接続要求を送る。この接続要求に対して、ＳＳＬサーバ１０は、サーバ証明書Ｓを接続要求元のクライアント端末に送信する。そして、クライアント端末２０（ｉ）は、自身のブラウザに埋め込まれたＣＡ証明書Ｒの情報を用いてＳＳＬサーバ１０から送られてきたサーバ証明書Ｓの検証を行う。この検証は、次のようにして行われる。

【００４０】図4に示すように、まず、受信したサーバ証明書Ｓの証明書本体における発行者Ｒと保存しているＣＡ証明書Ｒの証明書本体における主体者Ｒとが一致するか否かを確認する（破線参照）。それらが一致する場合、受信したサーバ証明書Ｓの検証に当該ＣＡ証明書Ｒの情報を使用できることが確認される。次に、サーバ証明書Ｓの証明書本体を、暗号化する際のアルゴリズムと同じアルゴリズムに従ってハッシュ処理してダイジェストを作成する。また、サーバ証明書Ｓに添付された電子署名を作成した際に用いられた秘密鍵R_{ks}と対になる公開鍵R_{kp}をＣＡ証明書Ｒの証明書本体から取得する。そして、この公開鍵R_{kp}を用いてサーバ証明書Ｓに添付された電子署名を復号してダイジェストを生成する（実線参照）。

【００４１】上記サーバ証明書Ｓの証明書本体からハッシュ処理にて作成したダイジェストと、上記電子署名を復号することにより生成されたダイジェストが一致するか否かを確認する（証明書の検証）。もし、それらのダイジェストが一致していなければ、受信したサーバ証明書ＳがＣＡ局３０から発行されたものと異なることであり、クライアント端末２０（ｉ）は、接続先のＳＳＬサーバ１０が不正なサービス提供者であるとしてその接続を中断することができる。

【００４２】一方、上記双方のダイジェストが一致する場合、クライアント端末２０（ｉ）は、接続先のＳＳＬサーバ１０がＣＡ局３０にて保証された正規のサービス提供者であるとして、以後、ＳＳＬサーバ１０に対してサービス提供に係る通信を続行する。

【００４３】上記サーバ証明書Ｓには前述したように有効期間が設定されており、その有効期間の期限が過ぎたサーバ証明書Ｓでは、クライアント端末において正規のサービス提供者であることの認証がとれないようになっている。そのため、ＳＳＬサーバ１０の管理者は、サービス提供の切れ目が発生しないように、ＣＡ局３０に対してサーバ証明書Ｓの発行依頼を行っている。また、ＳＳＬサーバ１０は、常に有効期限内のサーバ証明書Ｓにて運用が可能となるように保有する証明書の管理を行っ

11

ている。ＣＰＵ１１０での処理により実現されるこのＳＳＬサーバ１０の機能構成は、例えば、図5に示すようになっている。

【００４４】図5において、ＳＳＬサーバ１０は、有効期限監視部１２、証明書追加部１４、証明書削除部１６、登録状況管理部１５及び接続情報管理部１８を有している。登録状況管理部１５は、ＳＳＬサーバ１０に登録されている証明書の状況（有効期限、使用の有無など）を管理する。有効期限監視部１２は、登録状況管理部１５に登録された証明書の有効期限の管理を行う。証明書追加部１４は、新たな証明書を追加するための処理を行う。証明書削除部１６は、必要のなくなった証明書を削除するための処理を行う。

【００４５】上記のようにして接続要求のあったクライアント端末においてサーバ証明書Sに基づいた認証確認がなされた後に、接続情報管理部１８は、その接続要求のあったクライアント端末とＳＳＬプロトコルを用いた暗号通信を行うために必要な各種情報（暗号化種別、鍵情報、通信シーケンス番号など）からなる接続情報を生成して保持する。そして、この接続情報管理部１８に格納された接続情報に基づいて、ＳＳＬサーバ１０はその接続要求のあったクライアント端末（ブラウザ）とネットワーク５０を介して暗号通信を行う。この暗号通信においてＳＳＬサーバ１０らクライアント端末に対してサービスの提供（電子商取引など）がなされる。

【００４６】上記登録状況管理部１５は、例えば、図6に示すような証明書管理テーブルをを有し、ＳＳＬサーバ１０に登録された証明書の状況を管理する。この証明書管理テーブルは、補助記憶ユニット１６０に格納されている。図6（ａ）に示す証明書管理テーブルは、有効期間が1999．1．1～1999.12.31となる証明書Ｎｏ．０が登録され、その証明書Ｎｏ．０が現在使用中（○印）であることを表している。

【００４７】上記有効期限監視部１２は、例えば、図7に示す手順に従って処理を行う。

【００４８】図7において、内部タイマＴがスタートされた後（Ｓ１）に、いずれかのクライアント端末から接続要求があったか否かの確認（Ｓ２）及び内部タイマＴが所定時間Ｔｏ（例えば、1分間）に達したか否かの確認（Ｓ３）が行われる。内部タイマＴが上記所定時間Ｔｏに達すると、内部時計から現在時刻が取得される（Ｓ４）。そして、証明書管理テーブル（図6（ａ）参照）にて使用中のものとして管理される証明書Ｎｏ．０の有効期間（1999．1．1～1999.12.31）と上記取得した現在時刻とを比較して、現在使用中の証明書Ｎｏ．０の有効期限が切れているか否かが判定される（Ｓ５）。この証明書Ｎｏ．０の有効期限が切れていないと判定されると（Ｓ５でＹＥＳ）、更に、証明書管理テーブルを参照して、有効期間が現在使用中の証明書Ｎｏ．０の有効期間とオーバーラップすると共にその有効期限が現在使用中

12

の証明書Ｎｏ．０より先となる他の証明書があるか否かが判定される（Ｓ６）。ここで、そのような他の証明書がない場合には（Ｓ６でＮＯ）、内部タイマＴがリセットされた後（Ｓ７）、再度、内部タイマＴがスタートされ（Ｓ１）、上述した処理（Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６、Ｓ７）が実行される。

【００４９】上記のような手順により、所定時間Ｔｏ（例えば、１分間）毎に、現在使用中の証明書Ｎｏ．０の有効期限が切れているか否かのチェックが繰返し実行される。更に、そのようなチェックの繰返しの過程で、クライアント端末から接続要求があると（Ｓ２でＹＥＳ）、その場合にも上記と同様の手順（Ｓ４、Ｓ５、Ｓ６、Ｓ７）に従って、使用中の証明書Ｎｏ．０の有効期限が切れているか否かのチェックが行われる。これにより、周期的（例えば、1分間ごと）に行われるチェックでは検出できない証明書の有効期限切れが証明書を実際に必要とするとき（クライアント端末からの接続要求時）に検出できるようになる。

【００５０】例えば、図6（ａ）に示すように、証明書管理テーブルにおいて有効期間1999．1．1～1999.12.31の証明書Ｎｏ．０が使用中（○印）の証明書として管理されている場合、1999．1．1～1999.12.31の期間内では、上述した処理の結果、当該証明書Ｎｏ．０は、常に有効な（期限切れでない）証明書として確認される。その結果、ＳＳＬサーバ１０は、この有効な証明書Ｎｏ．０を用いて運用される。即ち、図5に示すように、各クライアント端末（ブラウザ）２０（ｉ）からの接続要求に対して、証明書Ｎｏ．０が有効な状態で作成された接続情報（情報群0：暗号種別、鍵情報、通信シーケンスなど）に基づいて暗号通信が行われる。

【００５１】また、上記のように証明書Ｎｏ．０での運用の過程で、当該証明書Ｎｏ．０の有効期限（1999.12.31）が近づくと、ＳＳＬサーバ１０の管理者はＣＡ局３０に対して新たな証明書Ｎｏ．１を発行するように要求する。そして、その新たな証明書Ｎｏ．１がＣＡ局３０から発行されると、その証明書Ｎｏ．１（図4におけるサーバ証明書S参照）がＳＳＬサーバ１０の補助記憶ユニット１６０に格納される。また、証明書追加部１４により当該証明書Ｎｏ．１の登録が行われる。この証明書追加部１４は、例えば、図8に示す手順に従って処理を行う。

【００５２】図8において、ＳＳＬサーバ１０の管理者が入力ユニット１４０を使用して新たな証明書Ｎｏ．１に関する証明書追加コマンドを入力すると、その証明書追加コマンドが取得されると共に（Ｓ２１）、内部時計から現在時刻が取得される（Ｓ２２）。更に、新たな証明書Ｎｏ．１の有効期間が取得される（Ｓ２３）。そして、その新たな証明書Ｎｏ．１の有効期間と現在時刻を比較して、現在時刻が有効期限の前であるか（有効期間が適正であるか）否かの判定が行われる（Ｓ２４）。こ

こで、現在時刻が有効期限の前(有効期間が適正) であると判定されると(Ｓ２４でＹＥＳ) 、その新たな証明書Ｎｏ．１の追加登録が行われる(Ｓ２５) 。 この証明書のＮｏ．１の追加登録は、証明書管理テーブルにこの証明書Ｎｏ．１を登録することによりなされる。この証明書Ｎｏ．１の有効期間が2000．1．1～2000.12.31となる場合、図6 (ｂ) に示すように、有効期間が1999.1.1～1999.12.31となる証明書Ｎｏ．０が既に登録されている証明書管理テーブルに、当該証明書Ｎｏ．１が追加登録される。そして、現在証明書Ｎｏ．０が使用されている状態であるので、証明書Ｎｏ．１は、使用されていない証明書として管理される(×印) 。

【００５３】なお、図8 に示す処理において、現在時刻が追加すべき証明書の有効期限の後となる(有効期間が適正でない) 場合、表示ユニット１３０にその旨のコメントが表示され(Ｓ２６) 、管理者からの指示入力の待ち状態となる(Ｓ２７) 。そして、管理者が表示ユニット１３０に表示されるコメントを確認して、入力ユニット１４０にて指示操作(追加登録キャンセル、強制追加登録、処理終了など) を行うと、その指示操作に従った処理が実行された後に、当該証明書追加登録に係る処理が終了する。

【００５４】上記のようにして新たな証明書Ｎｏ．１の追加登録がされた状態でも、既に登録されている証明書Ｎｏ．０の有効期間が残っている場合には、図7 に示す有効期限監視に係る処理において、使用中証明書Ｎｏ．０の有効期限が切れていないと判断される(図7 におけるＳ５でＹＥＳ) 。このため、図１０に示すように、各クライアント端末(ブラウザ) ２０(ｉ) からの接続要求に対して、証明書Ｎｏ．０が有効な状態で作成された接続情報(情報群0 : 暗号種別、鍵情報、通信シーケンスなど) に基づいて暗号通信が行われる。

【００５５】上記のようにして証明書Ｎｏ．０と追加登録された証明書Ｎｏ．１とが管理されている状態(図6 (ｂ) 参照) で、証明書Ｎｏ．０の有効期間の満了(1999.12.31) 直前にクライアント端末から接続要求がなされると、上記のようにこの証明書Ｎｏ．０が有効な状態で作成された接像情報に基づいてＳＬＬサーバ１０とその接続要求の要求元となるクライアント端末との間で暗号通信が行われる。そして、その暗号通信がなされている間に証明書Ｎｏ．０の有効期間が満了してもその暗号通信の状態(電子商取引を行っている状態) は維持される。

【００５６】一方、上記証明書Ｎｏ．０の有効期間の満了後(2000．1．1の0時以降) 、上述した所定周期Ｔｏ毎またはクライアント端末からの接続要求があったときになされる証明書の有効期限のチェック処理(図7 参照) では、使用中として管理されている証明書Ｎｏ．０の有効期限が切れていると判定される(Ｓ５においてＮＯ) 。すると、更に、有効となる他の証明書があるか否

かが判定される(Ｓ８) 。この場合、有効期間が2000．1．1～2000.12.31となる証明書Ｎｏ．１が登録されているので(図6 (ｂ) 参照) 、有効となる他の証明書Ｎｏ．１があると判定される。このように有効となる他の証明書Ｎｏ．１が登録されていると、証明書の置き換えの処理が行われる(Ｓ９) 。この証明書の置き換えの処理では、図6 (ｃ) に示すように、証明書管理テーブルにおいて、有効でなくなった証明書Ｎｏ．０の使用中が解除される(×印) と共に、有効となる新たな証明書Ｎｏ．１が使用中(○印) にされる。そして、内部タイマＴがリセットされた(Ｓ７) 後に、この使用中として管理される新たな証明書Ｎｏ．１に対して、前述したのと同様の手順(Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６、Ｓ７) に従って有効期限の監視がなされる。

【００５７】そして、図１１に示すように、上記のように証明書Ｎｏ．０が有効であったときにクライアント端末２０(１) 、２０(２) との間で開始された暗号通信が継続された状態で他のクライアント端末２０(ｊ) からＳＳＬサーバ１０に対して接続要求がなされると、使用中として新たに管理される証明書Ｎｏ．１がそのクライアント端末２０(ｊ) に送信されて当該ＳＳＬサーバ１０の認証確認が行われと共に、その新たな証明書Ｎｏ．１が有効となる状態で作成された接続情報(情報群１) に基づいてＳＳＬサーバ１０と当該クライアント端末２０(ｊ) との間で暗号通信が開始される。

【００５８】上記のような証明書の置き換えの処理により、ＳＳＬサーバ１０は、クライアント端末２０(１) 、２０(２) に対するサービス提供を継続させた状態で、有効となる証明書の置き換え(変更) を行うことが可能となる。そして、その証明書の置き換えが終了した後は、ＳＳＬサーバ１０はその新たな証明書を用いて運用される。

【００５９】なお、上述したような証明書の有効期限の監視処理(図7 参照) において、１つの証明書の有効期間が満了する前に、新たな証明書の追加登録がなされなかった場合、即ち、使用中として管理される証明書の有効期限が切れていると判定され(Ｓ５でＮＯ) 、かつ、有効となる他の証明書がないと判定された場合(Ｓ８でＮＯ) 、所定のエラー処理が実行されて、証明書の監視処理が終了する。その後、新たな証明書の登録がなされるまで、ＳＳＬサーバ１０は、サービス提供の業務を停止する。

【００６０】上記のように管理される証明書の有効期限切れが発生した後に、管理者は、その有効期限切れの証明書を削除することができる。この証明書削除に関する処理は、証明書削除部１６によってなされる。この証明書削除部１６は、例えば、図9 に示す手順に従って処理を実行する。

【００６１】図9 において、ＳＳＬサーバ１０の管理者が入力ユニット１４０を使用して有効期限の切れた削除

15

すべき証明書Ｎｏ．０に関する削除コマンドを入力すると、その削除コマンドが取得されると共に（Ｓ４１）、内部時計から現在時刻が取得される（Ｓ４２）。更に、その削除すべき証明書Ｎｏ．０の有効期間（1999.1.1～1999.12.31）が取得される（Ｓ４３）。そして、その有効期間と現在時刻を比較して、現在時刻が有効期限（1999.12.31）の後であるか（有効期間が不適切であるか）否かの判定が行われる（Ｓ４４）。ここで、現在時刻が有効期限の後（有効期間が不適切）であると判定されると（Ｓ４４でＹＥＳ）、その証明書Ｎｏ．０の削除が行われる（Ｓ４５）。即ち、証明書管理テーブルからこの証明書Ｎｏ．０の項目が削除されると共に、補助記憶ユニット１６０に格納された証明書Ｎｏ．０が削除される。その結果、証明書管理テーブルには、図6（ｄ）に示すように、現在使用中の証明書Ｎｏ．１だけが残り、以後、この証明書Ｎｏ．１の管理が継続して行われる。

【００６２】この状態で、各クライアント端末２０（ｉ）から接続要求がなされると、使用中として管理される証明書Ｎｏ．１が各クライアント端末２０（ｉ）に送信されて認証確認がなされる。そして、図１２に示すように、ＳＳＬサーバ１０は、この証明書Ｎｏ．１が有効となる状態で作成された接続情報（情報群1）に基づいて各クライアント端末２０（ｉ）と暗号通信を行う。

【００６３】なお、図9に示す処理において、現在時刻が削除すべき証明書の有効期限前となる（有効期間が適正である）場合、表示ユニット１３０に警報メッセージが表示されると共に、再度の削除コマンドの要求メッセージが表示される（Ｓ４６）。そして、ＳＳＬサーバ１０（ＣＰＵ１１０）は、管理者からの削除コマンドの再入力待ち状態になる（Ｓ４７）。この状態で、管理者が入力ユニット１４０を用いて削除コマンドを入力すると、指定された証明書の項目が証明書管理テーブルから削除されると共に、その証明書が補助記憶ユニット１６０から削除される（Ｓ４５）。

【００６４】なお、上述した例では、ユーザ（管理者）からの削除コマンドに基づいて有効期限が切れた証明書の削除がなされたが、有効期限の監視処理において、有効期限の切れた証明書が検出されたときに、自動的にその証明書を削除することもできる。

【００６５】また、上述した例では、新たに追加登録する証明書Ｎｏ．１の有効期間（2000.1.1～2000.12.31）は、使用中の証明書Ｎｏ．０の有効期間（1999.1.1～1999.12.31）とオーバーラップしていない。しかし、使用中の証明書Ｎｏ．０の有効期限が近づいたときに、その証明書Ｎｏ．０の有効期間とオーバーラップする有効期間となる証明書Ｎｏ．１を追加登録することもできる。

【００６６】例えば、図１３（ａ）に示すように、有効期間が1999.1.1～1999.12.31の証明書Ｎｏ．０が使用

16

中として管理されている状態で、上記有効期間とオーバーラップする有効期間1999.12.1～2000.12.31を有する新たな証明書Ｎｏ．１が図8に示す手順に従って追加登録されると、図１３（ｂ）に示すように、既に登録されている証明書Ｎｏ．０が使用中（○印）、追加登録された証明書Ｎｏ．１が未使用（×印）として管理される。現在時刻がこの未使用として管理される証明書Ｎｏ．１の有効期間の開始日になっていなければ、前述した場合と同様に、ＳＳＬサーバ１０は、証明書Ｎｏ．０を用いて運用される。

【００６７】一方、現在時刻がこの未使用の証明書Ｎｏ．１の有効期間の開始日（1999.12.1）以降になると、図7に示す有効期限の監視処理において、使用中の証明書Ｎｏ．０の有効期限が切れていないと判定される（Ｓ５でＹＥＳ）と共に、その有効期限が先となる有効な他の証明書Ｎｏ．１があると判定される（Ｓ６でＹＥＳ）。この場合、使用中の証明書Ｎｏ．０は有効ではあるが、証明書の置き換えの処理（Ｓ９）が行われる。その結果、図１３（ｃ）に示すように、証明書管理テーブルにおいて使用中であった証明書Ｎｏ．０の使用中が解除（未使用）され、新たな証明書Ｎｏ．１が使用中の状態に設定される。以後、この使用中として管理される証明書Ｎｏ．１を用いてＳＳＬサーバ１０の運用が行われる。

【００６８】このように、使用中の証明書の有効期間とオーバーラップする有効期間を有する証明書の追加登録がなされて、その追加登録された証明書の有効期間の開始日になると、使用中であった証明書の有効期間が残っていても、強制的に追加登録された証明書での運用が開始されるので、常に最新の証明書を用いたＳＳＬサーバ１０の運用が可能となる。

【００６９】なお、上記のようにして有効期間内であるにもかかわらず未使用として管理されるようになった証明書Ｎｏ．０に対する削除コマンドが入力されると、前述したように、図9に示す処理において、表示ユニット１３０に警報メッセージと削除コマンドの再入力の要求メッセージが表示される（Ｓ４６）。そして、管理者が入力ユニット１４０を用いて削除コマンドの再入力を行うと（Ｓ４７でＹＥＳ）、この有効期間のまだ残っている証明書Ｎｏ．０の削除処理が行われる（Ｓ４５）。そして、以後、追加登録された証明書Ｎｏ．１だけが、図１３（ｄ）に示すように、証明書管理テーブルにおいて使用中の証明書として管理される。

【００７０】上述した例において、図6及び図１３に示す証明書管理テーブルが証明書管理手段に対応し、図7に示す手順での処理が管理変更制御手段に対応する。また、証明書追加部１４での処理（図8参照）が証明書追加手段に対応し、証明書削除部１６での処理（図9参照）が証明書削除手段に対応する。

【００７１】

17

【発明の効果】以上、説明してきたように、請求項1乃至9に記載された本願発明によれば、所定のタイミングで、認証に使用されることなく保存される電子証明書の管理を上記認証に使用されるべき電子証明書としての管理に変更すると共に、上記認証に使用されるべき電子証明書の管理を上記認証に使用されることなく保存される電子証明書の管理に変更するようになるので、サービス提供サーバの運用を継続した状態で認証に使用されるべき電子証明書の変更を行うことのできるようになる。

【００７２】また、請求項１０及び１１記載の本願発明によれば、上記のような電子証明書の管理方法に従った処理をコンピュータに行わせるためのプログラム及びそれを格納した記憶媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施の一形態に係る電子証明書の管理方法が適用されるシステムの基本的な構成を示すブロック図である。

【図2】図1に示すＳＳＬサーバのハードウエア構成の一例を示すブロック図である。

【図3】ＣＡ局にて発行される各証明書の関係の一例を示す図である。

【図4】ＣＡ局にて発行される各証明書の内容の一例を示す図である。

【図5】ＳＳＬサーバの機能構成の一例及びＳＳＬサーバの状態（その１）を示すブロック図である。

【図6】証明書管理テーブルの遷移状態の一例を示す図である。

18

【図7】有効期限監視部での処理手順の一例を示すフローチャートである。

【図8】証明書追加部での処理手順の一例を示すフローチャートである。

【図9】証明書削除部での処理手順の一例を示すフローチャートである。

【図１０】ＳＳＬサーバの状態（その２）を示す図である。

【図１１】ＳＳＬサーバの状態（その３）を示す図である。

【図１２】ＳＳＬサーバの状態（その４）を示す図である。

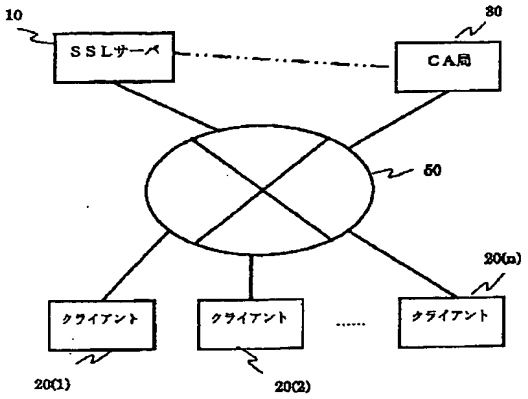
【図１３】証明書管理テーブルの遷移状態の他の一例を示す図である。

【符号の説明】

１０　ＳＳＬサーバ（サービス提供サーバ）
２０（１）、２０（２）、…、２０（ｎ）　クライアント端末
３０　ＣＡ局（認証局）
１１０　ＣＰＵ
１２０　メモリユニット
１３０　表示ユニット
１４０　入力ユニット
１５０　通信ユニット
１６０　補助記憶ユニット
１７０　ＣＤ－ＲＯＭドライバユニット
１８０　ＣＤ－ＲＯＭ

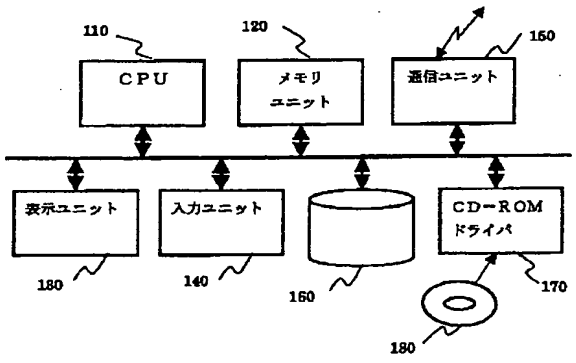
【図1】

本発明の実施の一形態に係る電子証明書の管理方法が適用されるシステムの基本的な構成を示すブロック図



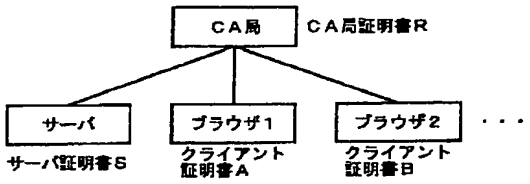
【図2】

図1に示すＳＳＬサーバのハードウエア構成の一例を示すブロック図



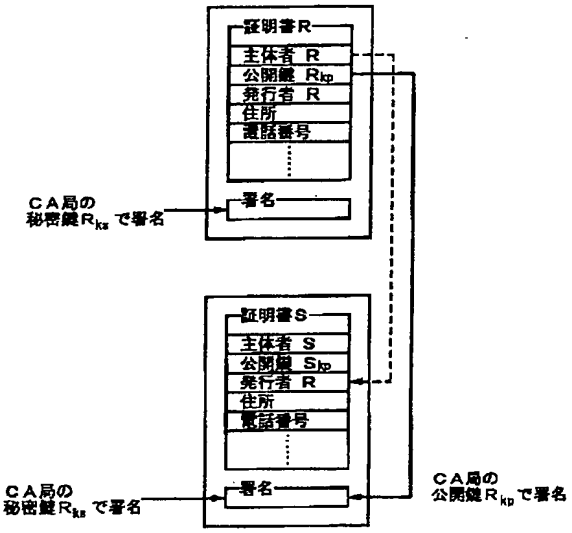
【図3】

ＣＡ局にて発行される各証明書の関係の一例を示す図



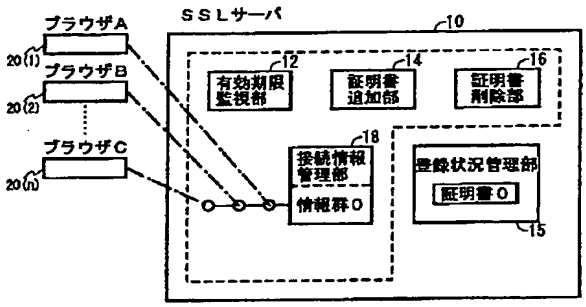
【図4】

ＣＡ局にて発行される各証明書の内容の一例を示す図



【図5】

ＳＳＬサーバの機能構成の一例及び
ＳＳＬサーバの状態（その１）を示すブロック図



【図6】

証明書管理テーブルの遷移状態の一例を示す図

(a)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	○

(b)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	○
Ｎｏ．１	2000.1.1 ～ 2000.12.31	×

(c)

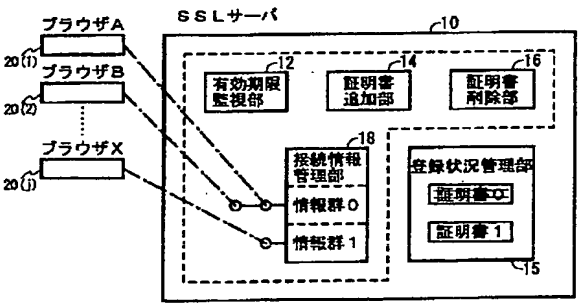
証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	×
Ｎｏ．１	2000.1.1 ～ 2000.12.31	○

(d)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．１	2000.1.1 ～ 2000.12.31	○

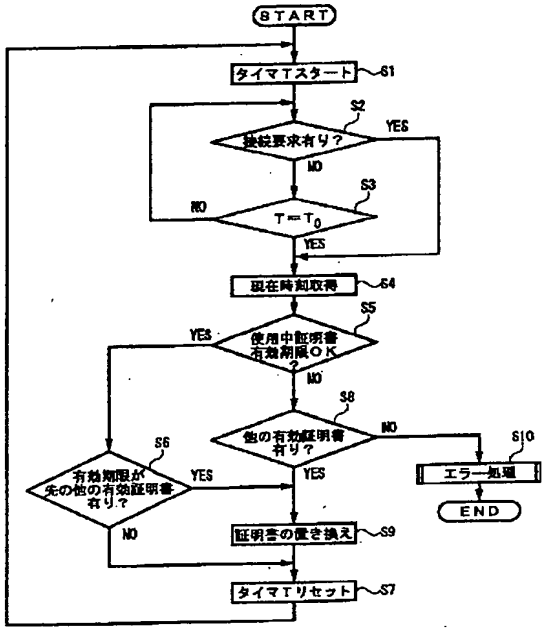
【図11】

ＳＳＬサーバの状態（その３）を示す図



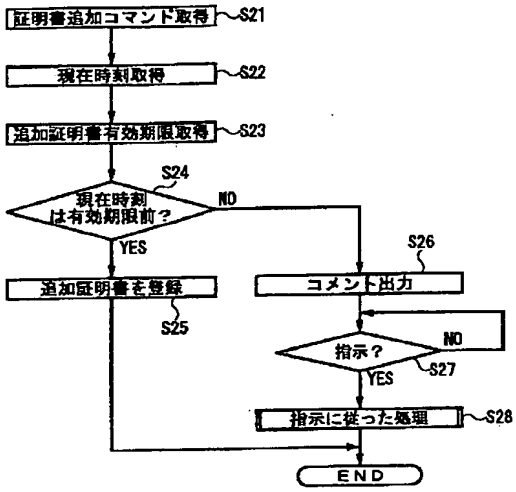
【図７】

有効期限監視部での処理手順の一例を示すフローチャート



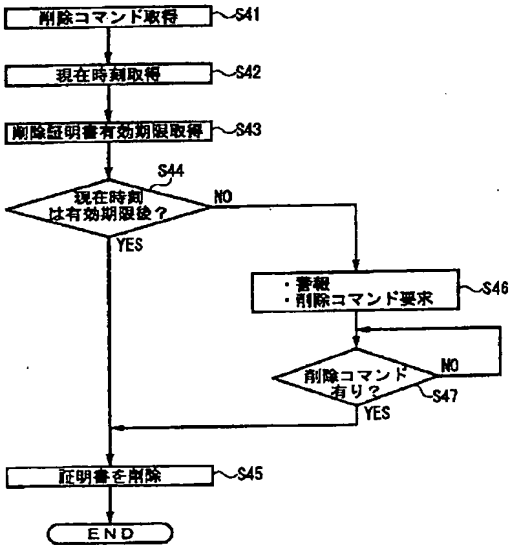
【図８】

証明書追加部での処理手順の一例を示すフローチャート



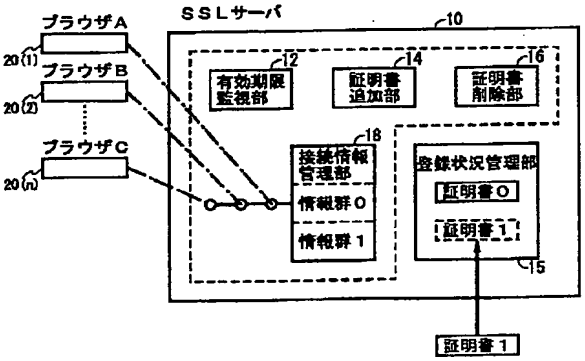
【図９】

証明書削除部での処理手順の一例を示すフローチャート



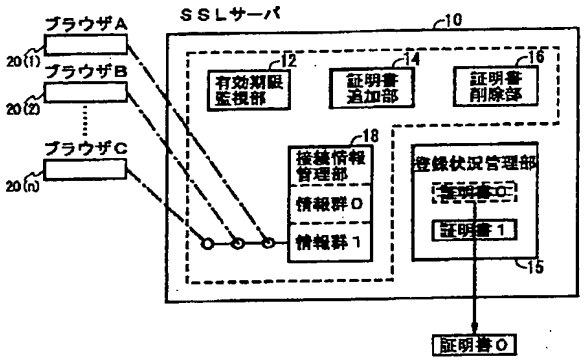
【図１０】

ＳＳＬサーバの状態（その２）を示す図



【図１２】

ＳＳＬサーバの状態（その４）を示す図



【図１３】

証明書管理テーブルの遷移状態の他の一例を示す図

(a)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	○

(b)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	○
Ｎｏ．１	1999.12.1～ 2000.12.31	×

(c)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．０	1999.1.1 ～ 1999.12.31	×
Ｎｏ．１	1999.12.1～ 2000.12.31	○

(d)

証明書Ｎｏ.	有効期間	使用中
Ｎｏ．１	1999.12.1～ 2000.12.31	○